

# Succendo 制造业解决方案

## 制造业需求分析

随着制造业企业大量使用信息技术来提高整个企业的竞争力和生产效率，制造业企业管理开始面临关于企业的物流、资金流、信息流等开始实现信息化的问题，像 OA、ERP、MRP、SCM、CRM 等概念和产品非常流行。为了能够让遍布在全国各地的分支机构方便地使用 ERP 等系统，确保总部对各项数据进行统一的协调和管理，制造业企业希望选取一种高效、安全、稳定的远程接入解决方案，提升企业运营效率并保证未来的健康发展。不过无论选择那一种应用模式，安全可靠的远程访问网络系统的搭建都是必不可少的。

SSL VPN 是基于应用层的 VPN，这就意味着在安全性上已经不仅局限在可以让数据安全传输过来，而且还关注传输过来的数据究竟是什么内容。对于企业而言，采用 SSL VPN，不仅可以让外地员工对 Web 化的 ERP 应用进行访问，而且可以知道访问 ERP 应用的数据连接究竟是由哪个员工发起、他或者她究竟有哪些权限来进行操作。

由于客户端与 SSL VPN 网关之间实现高强度的加密信息传输，因此虽然信息传输是通过公网进行的，但是其安全性是可以得到保证的。第三方即使可以得到传输数据，但是却无法得到隐藏在其中的明文信息。

SSL VPN 的访问要经过认证和授权，充分保证用户身份的合法性。如果请求连接的用户没有合法身份，则 SSL VPN 将拒绝其连接请求，从而限制了非法用户对内网的访问。

SSL VPN 方案实施起来非常简单，只需要在企业的防火墙后部署 SSL VPN 网关即可，无需在各分支机构部署硬件或软件设备。SSL VPN 方案是无客户端的 VPN 方案，客户端只需要具备标准的浏览器即可。SSL VPN 的管理工作属于集中管理和集中维护模式，可以极大地降低管理和维护成本。

## 安全方案设计原则

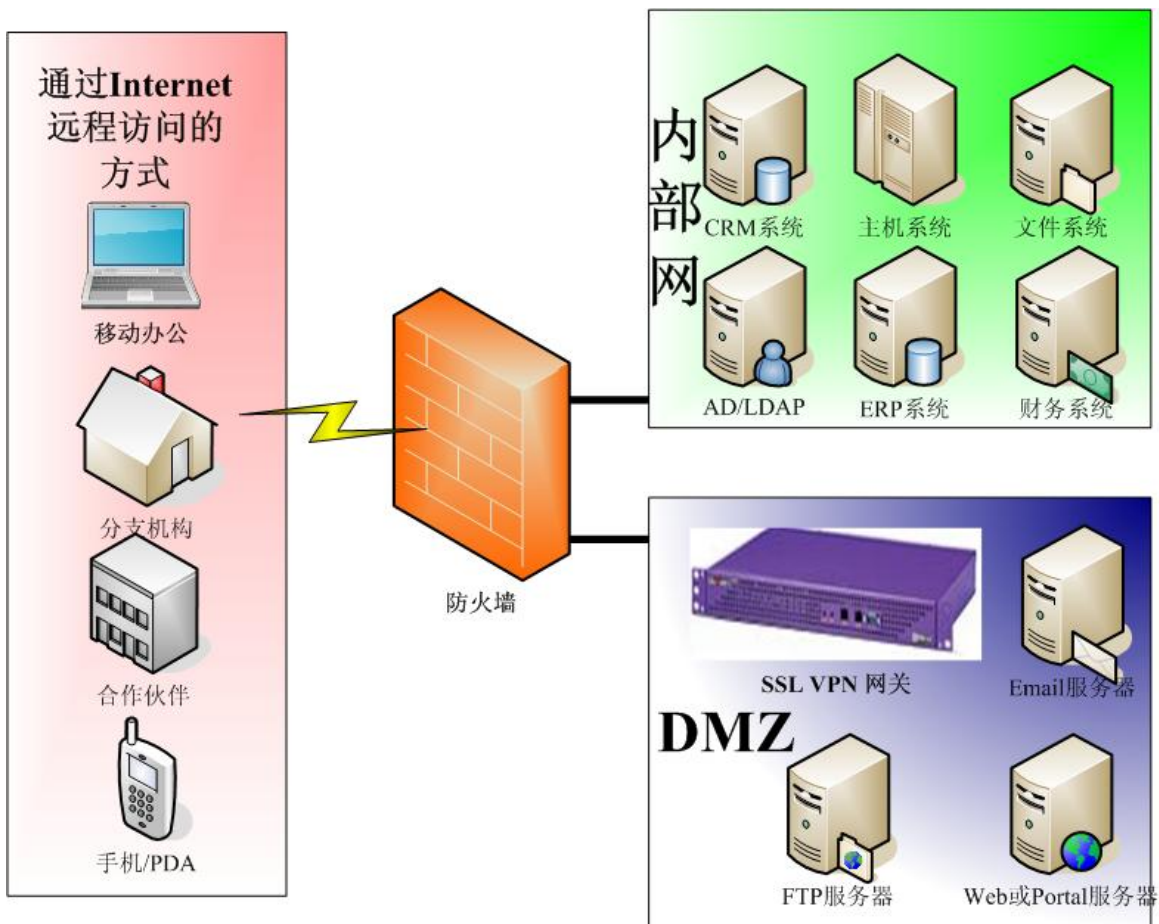
- ❖ 需求、风险、代价平衡分析的原则：对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定系统的安全策略。
- ❖ 综合性、整体性原则：运用系统工程的观点、方法，分析网络的安全问题，并制定具体措施。
- ❖ 一致性原则：网络安全问题应与整个网络的工作周期同时存在，制定的安全体系结构必须与网络的安全需求相一致。
- ❖ 易操作性原则：措施过于复杂，对人的要求过高，本身就降低了安全性。
- ❖ 适应性、灵活性原则：能随着网络性能及安全需求的变化而变化，要容易适应、容易修改。
- ❖ 多重保护原则：建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其它层保护仍可保护信息的安全。

## 产品选型原则

- ❖ 加密通讯：主动的加密通讯，可使攻击者不能了解、修改敏感信息；

- ❖ 认证：良好的认证体系可防止攻击者假冒合法用户；
- ❖ 隐藏内部信息：使攻击者不能了解系统内的基本情况；
- ❖ 安全监控中心：为信息系统提供安全体系管理、监控，保护及紧急情况服务。
- ❖ 适用大多数设备：基于 Web 访问的开放体系可以被任何运行标准浏览器的系统所访问，包括非传统设备，如可以上网的手机和 PDA 通信产品。
- ❖ 适用于大多数操作系统：不管是 Windows、Macintosh、UNIX 还是 Linux，只要运行标准的浏览器，都可以支持 SSL VPN 对企业内部网站和 Web 站点进行访问。
- ❖ 良好的安全性：SSL VPN 访问的并不是网络的真实节点，而是被代理的内部资源，这种方法较为安全。
- ❖ 较强的资源控制能力：SSL VPN 为远程访问用户提供较细粒度的资源访问控制。
- ❖ 绕过防火墙和代理服务器：基于 SSL VPN 的远程访问方案可以绕过防火墙和代理服务器访问企业网资源

网络安全规划示意拓扑图



如图所示，在企业内部网的防火墙的 DMZ 区部署 **Succendo VPN 网关**。当用户通过 **SSL VPN** 访问内网资源的时候，直接访问到的是 **Succendo VPN 网关**，用户的访问请求和数据将由 **Succendo VPN 网关** 转发。这样就为为远程访问的用户提供安全的访问企业内部网资源的 VPN 通道，并保证了企业内部网的安全性。

经过用户的实际使用和测试，**Succendo VPN 网关**能够高效、安全、稳定的远程接入解决方案，提升企业运营效率并保证未来的健康发展，节省了大量专线的费用。事实证明，**Succendo VPN 网关**能够为制造业企业的信息化应用保驾护航。